FIBONACCI SYSTEM AND RESIDUE COMPLETENESS

Cheng Lien Lang and Mong Lung Lang

Abstract. A Fibonacci cycle $C(a, b, \mathbb{Z}_m)$ is residue complete (nondefective) if and only if $\gcd(b^2 - ab - a^2, m) = 1$ and $m \in \{5^k, 2 \cdot 5^k, 4 \cdot 5^k, 3^j 5^k, 6 \cdot 5^k, 7 \cdot 5^k, 14 \cdot 5^k \mid k \geq 0, j \geq 1\}$. In particular, the Lucas numbers modulo m is residue complete if and only if $m = 2, 4, 6, 7, 14, 3^n$ $(n \geq 1)$.

1. Introduction

Denoted by F_n the n-th Fibonacci number ($F_0 = 0, F_1 = F_2 = 1, \cdots, F_{n+1} = F_n + F_{n-1}$). It is well known that

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \sigma^n = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \in GL(2, \mathbb{Z}). \tag{1.1}$$

Let m be a positive integer. The Fibonacci numbers modulo m form a subset of $\mathbb{Z}_m$. The number m is *defective* if the Fibonacci numbers is not a complete system of residues modulo m. In [B], the author studied the structure of the Fibonacci system modulo m and completely characterised all defective and nondefective (residue complete) moduli. In the same paper, the author suggested that one should give a systematic study of the Fibonacci system modulo m. In this article, we took his advice and study the Fibonacci system modulo m. Our main result can be found in Proposition 7.2 which completely characterised all residue complete Fibonacci cycles modulo m. In particular, Lucas numbers modulo m is residue complete if and only if $m = 2, 4, 6, 7, 14, 3^n$ $(n \geq 1)$. We would also like to take this opportunity to offer an alternative proof of Lemma 2 of [B] as the original proof involves some misprint (the equation $2^2 + 2b - b^2 \equiv -1$ in pp 501 of [B] is not solvable modulo 9). The proof we presented here in Lemma 6.4 is actually the same as [B]. The only difference is that one needs to consider two cases rather than one.

Sections 2 to 5 give basic properties about the Fibonacci system and Sections 6 and 7 are devoted to the characterisation of Fibonacci cycles that are residue complete.

2. Fibonacci system of $\mathbb{Z}_m$.

For each nonzero pair $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_m$, define the following sequence modulo m.

$F(a, b, \mathbb{Z}_m) = \{E_1 = a, E_2 = b, E_3 = b + a = E_2 + E_1, \cdots, E_{n+1} = E_n + E_{n-1}, \cdots\}$.

One sees easily that $E_{n+1} = bF_n + aF_{n-1}$. Let $E_0 = b - a$. By (1.1), one has

$$\begin{pmatrix} b & a \\ a & b - a \end{pmatrix} \sigma^n \equiv \begin{pmatrix} E_{n+2} & E_{n+1} \\ E_{n+1} & E_n \end{pmatrix}. \tag{2.1}$$

2000 *Mathematics Subject Classification.* 11B39.

Key words and phrases. Fibonacci numbers.

for all $n \geq 0$. Note that $F(0,1,\mathbb{Z}_m)$ is just the Fibonacci numbers modulo m. It is clear that $F(a,b,\mathbb{Z}_m)$ is periodic. Denoted by $C(a,b,\mathbb{Z}_m)$ a period of this sequence and called it the *Fibonacci cycle* associated to (a,b). Two periods $C(a,b,\mathbb{Z}_m)$ and $C(c,d,\mathbb{Z}_m)$ are *equivalent* if one can be obtained from the other by a cyclic permutation. Following our definition, $C(1,3,\mathbb{Z}_5) = (1,3,4,2)$ and $C(2,1,\mathbb{Z}_5) = (2,1,3,4)$ are equivalent. It is clear that if (c,d) appears in $C(a,b,\mathbb{Z}_m)$, then $C(a,b,\mathbb{Z}_m) = C(c,d,\mathbb{Z}_m)$. In particular, one has $C(0,1,\mathbb{Z}_m) = C(1,1,\mathbb{Z}_m)$.

Definition 2.1. Let $C(a,b,\mathbb{Z}_m)$ be a Fibonacci cycle. Denoted by $k(a,b,\mathbb{Z}_m)$ the number of terms in $C(a,b,\mathbb{Z}_m)$. In the case $a = 0, b = 1$, we shall simply denote this number by $k(m) = k(0,1,\mathbb{Z}_m)$.

Lemma 2.2. *Let $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_m$ be a nonzero pair. Then $k(a,b,\mathbb{Z}_m)$ is the smallest positive integer such that*

$$\begin{pmatrix} b & a \\ a & b-a \end{pmatrix} \sigma^{k(a,b,\mathbb{Z}_m)} \equiv \begin{pmatrix} b & a \\ a & b-a \end{pmatrix}. \tag{2.2}$$

Further, (a) if $gcd(b^2 - ab - a^2, m) = 1$, then $k(a,b,\mathbb{Z}_m) = k(m)$ is the order of σ in $GL(2,\mathbb{Z}_m)$ (note that $b^2 - ab - a^2$ is the determinant of the matrix in (2.2)), (b) $k(a,b,\mathbb{Z}_m)|k(m)$.

Proof. Suppose that $k(a,b,\mathbb{Z}_m) = n$. Then $C(a,b,\mathbb{Z}_m) = (a,b,a+b,E_4,\cdots,E_n)$, $E_{n+1} \equiv a$, $E_{n+2} \equiv b$ and n is the smallest positive integer such that $E_{n+1} \equiv a$ and $E_{n+2} \equiv b$. Since $E_{n+2} = E_n + E_{n+1}$ and $E_{n+1} \equiv a$, $E_{n+2} \equiv b$, one has $E_n \equiv b - a$. An easy observation of (2.1) implies that $k(a,b,\mathbb{Z}_m)$ is the smallest positive integer such that (2.2) holds.
(a) and (b) can now be proved easily. Note that $k(m) = k(0,1,\mathbb{Z}_m)$. □

Definition 2.3. Let $F(a,b,\mathbb{Z}_m) = \{E_1, E_2, \cdots, E_t, \cdots\}$. Two adjacent terms (E_r, E_{r+1}) is called a *pair*. A pair (E_r, E_{r+1}) is called a *multiple* of (a,b) if $(E_r, E_{r+1}) = (ea, eb)$ for some unit $e \in \mathbb{Z}_m^\times$. Denoted by $\alpha(a,b,\mathbb{Z}_m)$ the smallest positive integer t such that $(E_{t+1}, E_{t+2}) = (eE_1, eE_2)$ for some unit $e \in \mathbb{Z}_m^\times$. In the case $a = 0, b = 1$, we shall simply denote this number by $\alpha(m) = \alpha(0,1,\mathbb{Z}_m)$.

Discussion 2.4. Basic properties about $k(m)$ and $\alpha(m)$ can be found in Appendix A. Remark of Appendix A indicates that the behavior of $k(a,b,\mathbb{Z}_m)$ and $\alpha(a,b,\mathbb{Z}_m)$ is less systematic than $k(m)$ and $\alpha(m)$. By Lemma 2.2 and Definition 2.3,

$$(b,a)\sigma^{k(a,b,\mathbb{Z}_m)} = (b,a),\ (b,a)\sigma^{\alpha(a,b,\mathbb{Z}_m)} = e(b,a). \tag{2.3}$$

Hence (b,a) is an eigenvector of $\sigma^{\alpha(a,b,\mathbb{Z}_m)}$ with eigenvalue e. This is the main reason that we consider the Fibonacci cycle $C(a,b,\mathbb{Z}_m)$ for nonzero pairs (a,b) only. We will show in Appendix B that if $(x,y) \in F(a,b,\mathbb{Z}_m)$ is a multiple of (a,b), then (x,y) can always be written as $e(a,b)$, where $e \in \mathbb{Z}_m$ is a unit.

Example 2.5. Let $E_1 = 2, E_2 = 2$. Then $C(2,2,\mathbb{Z}_6) = (2,2,4,0,4,4,2,0)$ and $(4,4) = (E_5, E_6) = x(E_1, E_2)$ for $x = 2, 5$. Since 5 is unit, we have $\alpha(2,2,\mathbb{Z}_6) = 4$.

Lemma 2.6. *Let $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_m$ be a nonzero pair. Then $\alpha(a,b,\mathbb{Z}_m)$ is the smallest positive integer such that*

$$\begin{pmatrix} b & a \\ a & b-a \end{pmatrix} \sigma^{\alpha(a,b,\mathbb{Z}_m)} \equiv e \begin{pmatrix} b & a \\ a & b-a \end{pmatrix} \tag{2.4}$$

for some unit e. Further, (a) if $gcd(b^2-ab-a^2, m) = 1$, then $\alpha(a, b, \mathbb{Z}_m) = \alpha(m) = \alpha(0, 1, \mathbb{Z}_m)$, (b) $\alpha(m)$ is the smallest positive integer such that $F_{\alpha(m)} \equiv 0 \ (mod\ m)$, $\alpha(a, b, \mathbb{Z}_m)|\alpha(m)$, $\alpha(m)|k(m)$.

Proof. Let $t = \alpha(a, b, \mathbb{Z}_m)$. Definition 2.3 and identity (2.1) imply that t is the smallest positive integer such that

$$\begin{pmatrix} b & a \\ a & b-a \end{pmatrix} \sigma^t \equiv e \begin{pmatrix} b & a \\ a & b-a \end{pmatrix} \equiv \begin{pmatrix} E_{t+2} & E_{t+1} \\ E_{t+1} & E_t \end{pmatrix}. \tag{2.5}$$

Suppose that $\gcd(b^2 - ab - a^2, m) = 1$. (2.5) implies that $\sigma^t \equiv eI \pmod m$. It follows that for any (a, b), as long as $\gcd(b^2-ab-a^2, m) = 1$, then $t = \alpha(a, b, \mathbb{Z}_m)$ is the smallest positive integer such that σ^t is an invertible scalar matrix. Since such t is determined uniquely by σ, we conclude that $\alpha(a, b, \mathbb{Z}_m) = \alpha(0, 1, \mathbb{Z}_m) = \alpha(m)$. This completes the proof of (a). Let $a = 0, b = 1$. (2.5) implies that $t = \alpha(m)$ is the smallest positive integer such that $E_{\alpha(m)+1} = F_{\alpha(m)} \equiv 0 \pmod m$. This completes the proof of the first part of (b). Since $E_{\alpha(m)+1} = F_{\alpha(m)} \equiv 0 \pmod m$, we have $F_{\alpha(m)+1} \equiv F_{\alpha(m)-1} \pmod m$. As a consequence,

$$\sigma^{\alpha(m)} \equiv \begin{pmatrix} F_{\alpha(m)-1} & 0 \\ 0 & F_{\alpha(m)-1} \end{pmatrix}. \tag{2.6}$$

Let $\alpha(m) = q\alpha(a, b, \mathbb{Z}_m) + r$, where q is the quotient and r is the remainder. (2.9) implies that $F_{\alpha(m)-1}(b, a) = e^q(b, a)\sigma^r$. Since $F_{\alpha(m)-1}$ and the eigenvalue e of $\sigma^{\alpha(a,b,\mathbb{Z}_m)}$ are units (see Definition 2.3), the minimality of $\alpha(a, b, \mathbb{Z}_m)$ implies that $r = 0$. Hence $\alpha(a, b, \mathbb{Z}_m)|\alpha(m)$. It is clear that $\alpha(m)|k(m)$. □

Let $C = C(a, b, \mathbb{Z}_m)$ be a Fibonacci cycle. We construct in the following two Fibonacci cycles, one for $\mathbb{Z}_m$ which we denoted by rC and one for $\mathbb{Z}_{tm}$ which we denoted by $t[C]$.

Lemma 2.7. *Suppose that $gcd(r, m) = 1$. Then $rC(a, b, \mathbb{Z}_m) = C(ra, rb, \mathbb{Z}_m) = (ra, rb, ra + rb, \cdots)$ is a Fibonacci cycle of $\mathbb{Z}_m$ and $k(a, b, \mathbb{Z}_m) = k(ra, rb, \mathbb{Z}_m)$. Let t be an integer, then $t[C(a, b, \mathbb{Z}_m)] = (ta, tb, \cdots)$ is a Fibonacci cycle of $\mathbb{Z}_{tm}$.*

Example 2.8. (i) $C(3, 3, \mathbb{Z}_9) = (3, 3, 6, 0, 6, 6, 3, 0) = 3[C(1, 1, \mathbb{Z}_3)] = (3x : x \in C(0, 1, \mathbb{Z}_3))$, where $C(1, 1, \mathbb{Z}_3) = (1, 1, 2, 0, 2, 2, 1, 0)$. (ii) Let $C = C(1, 4, \mathbb{Z}_{11}) = (1, 4, 5, 9, 3)$. Then $2C = C(2, 8, \mathbb{Z}_{11}) = (2, 8, 10, 7, 6)$.

Lemma 2.9. *The collection $FS(m)$ of all inequivalent Fibonacci cycles modulo m is called the* Fibonacci system *of $\mathbb{Z}_m$. The total number of terms appear in $FS(m)$ is $m^2 - 1$.*

Proof. Let (a, b) be a nonzero pair. By our definition of Fibonacci cycle, (a, b) must appear as adjacent terms in some Fibonacci cycles. Since the Fibonacci system consists of inequivalent Fibonacci cycles, the pair (a, b) appears exactly once in $FS(m)$. Our assertion now follows by the fact that there are exactly m^2-1 nonzero pairs in $\mathbb{Z}_m \times \mathbb{Z}_m$. □

Calculate the determinant of the matrices of (2.1), one has the following result.

Lemma 2.10. *For any $E_{n+1}, E_n \in C(a, b, \mathbb{Z}_m)$, $E_{n+1}^2 - E_{n+1}E_n - E_n^2 \equiv \pm(b^2 - ba - a^2) \ (mod\, m)$. Hence if $b^2 - ba - a^2 \neq \pm(d^2 - dc - c^2) \ (mod\, m)$, then $C(a, b, \mathbb{Z}_m)$ and $C(c, d, \mathbb{Z}_m)$ are not equivalent to each other.*

Definition 2.11. $\pm(b^2-ba-a^2) \pmod m$ is called the *discriminant* of $C(a,b,\mathbb{Z}_m)$.

Lemma 2.12. *Let $C \in FS(m)$. Then C consists of 0 if and only if $C = rC(0,m_0,\mathbb{Z}_m)$, where $gcd(r,m)=1$ and the set of prime divisors of m_0 is a subset of the set of prime divisors of m.*

Proof. Suppose that $0 \in C$. Then C takes the form $(\cdots,t,0,t,\cdots)$ for some t. Let $t = rm_0$, where r and m_0 are given as in the lemma. Then $C = rC(0,m_0,\mathbb{Z}_m)$ (see Lemma 2.7 for the notation $rC(0,m_0,\mathbb{Z}_m)$). The converse is clear. □

Definition 2.13. $\beta(a,b,\mathbb{Z}_m) = k(a,b,\mathbb{Z}_m)/\alpha(a,b,\mathbb{Z}_m)$. In the case $a=0$, $b=1$, we shall simply denote this number by $\beta(m) = \beta(0,1,\mathbb{Z}_m)$.

Remark 2.14. By Definition 2.3 and Discussion 2.4, $\beta(a,b,\mathbb{Z}_m)$ gives the number of pairs of $C(a,b,\mathbb{Z}_m)$ that are multiples of (a,b). In the case $C = C(a,b,\mathbb{Z}_m)$ consists zero, $\beta(a,b,\mathbb{Z}_m)$ tells us how many zeros C possess.

Lemma 2.15. *Suppose that $m \geq 3$, $gcd(b^2-ab-a^2,m)=1$. Then $k(a,b,\mathbb{Z}_m) = k(m)$, $\alpha(a,b,\mathbb{Z}_m) = \alpha(m)$ and $\beta(m) \leq 4$. Further,*

(i) *If $\alpha(m)$ is odd, then $\beta(m)=4$.*
(ii) *If $\alpha(m)$ is a multiple of 4, then $\beta(m)=2$.*
(iii) *If $\alpha(m)$ takes the form $4r+2$, then $\beta(m)=1$ or 2 and that $\beta(m)=2$ if and only if $k(m)$ is a multiple of 4.*

Proof. Note that $k(2)=\alpha(2)=3$, $\beta(2)=1$. By Lemmas 2.2 and 2.6, $k(a,b,\mathbb{Z}_m) = k(m)$ and $\alpha(a,b,\mathbb{Z}_m) = \alpha(m)$.

Since $k(m) = \alpha(m)\beta(m)$ is the order of σ modulo m, (2.6) implies that $\beta(m)$ is the smallest positive integer such that

$$(F_{\alpha(m)-1})^{\beta(m)} \equiv 1. \tag{2.7}$$

On the other hand, since the determinant of σ is -1, (2.6) gives

$$(-1)^{\alpha(m)} \equiv (F_{\alpha(m)-1})^2. \tag{2.8}$$

Since $m \geq 3$, $-1 \not\equiv 1 \pmod m$. It follows from (2.7) and (2.8) that $\beta(m)$ is a divisor of 4. We shall now prove (i)-(iii) as follows. Note first that we are work on the cycle $C(0,1,\mathbb{Z}_m) = (0,1,1,F_3,F_4,\cdots)$. (i) follows from the definition of $\beta(m)$ and (2.10), (2.11). We shall now prove (ii). Set $\alpha(m) = 4r$. By (2.7) and (2.8), $\beta(m) = 1$ or 2. Suppose that $\beta(m)=1$. Then $k(m) = \alpha(m) = 4r$. It follows that $C(0,1,\mathbb{Z}_m)$ has only one zero (see Remark 2.14), which is $F_0 = 0$. Since $k(m) = 4r$, one has $F_{4r} \equiv 0$, $F_{4r+1} \equiv 1 \pmod m$. Applying the identity $F_{n+1} = F_n + F_{n-1}$, one can show easily that $F_{4r-2k} \equiv -F_{2k}$ and $F_{4r-(2k+1)} \equiv F_{2k+1}$ for $k \leq r$. Hence $C(0,1,\mathbb{Z}_m)$ takes the form

$$\cdots, F_{2r-1}, F_{2r}, F_{2r+1} \equiv F_{2r-1}, \cdots \tag{2.9}$$

Since $F_{2r+1} = F_{2r} + F_{2r-1}$, one has $F_{2r} \equiv 0$. In particular, $\alpha(m) \leq 2r$. A contradiction ($\alpha(m) = 4r$). Hence $\beta(m) = 2$.

We shall now prove (iii). Set $\alpha(m) = 4r+2$. By (2.7) and (2.8), $\beta(m) = 1$ or 2. It is clear that if $k(m)$ is not a multiple of 4, then $\beta(m) = k(m)/\alpha(m) = 1$. We shall therefore assume that $k(m) = 4r$ is a multiple of 4. Since $\beta(m) = 1$ or 2, it follows easily that $\beta(m) = k(m)/\alpha(m) = 2$.

□

Remark 2.16. Lemma 2.15 actually tells us more than it looks. Take $k(m) = 8r$ for some r for example, since $k(m)/\alpha(m) = \beta(m) = 1, 2$ or 4, $\alpha(m)$ must be even. (ii) and (iii) together imply that $\alpha(m)$ must be a multiple 4. Consequently, $\beta(m) = 2$. □

Lemma 2.17. *Suppose that* $m|(b^2 - b - 1)$. *Then* $k(1, b, \mathbb{Z}_m) = \beta(1, b, \mathbb{Z}_m)$.

Proof. $C(1, b, \mathbb{Z}_m) = (1, b, b + 1, \cdots)$. Since $b^2 - b - 1$ is a multiple of m, one sees easily that $b(1, b) = (b, b + 1)$ and that b is a unit. Hence $\alpha(1, b, \mathbb{Z}_m) = 1$. This completes the proof our assertion. □

3. Fibonacci system of $\mathbb{Z}_{p^n}$

Discussion 3.1. Let $C = C(a, b, \mathbb{Z}_{p^n}) \in FS(p^n)$. Suppose that the discriminant of C is a multiple of p. Then $b^2 - ab - a^2$ is a multiple of p. Let p^r be the largest power of p that divides $\gcd(a, b)$. Then C takes the form $p^r[S]$, where $S = C(a/p^r, b/p^r, \mathbb{Z}_{p^{n-r}})$ (see Lemma 2.7 and Example 2.8). Let $a_0 = a/p^r, b_0 = b/p^r$. Then either a_0 or b_0 is a unit in $\mathbb{Z}_{p^{n-r}}$. It follows that $S = a_0 C(1, a_0^{-1} b_0, \mathbb{Z}_{p^{n-r}})$ if a_0 is a unit or $S = b_0 C(a_0 b_0^{-1}, 1, \mathbb{Z}_{p^{n-r}}) = b_0 C(1, a_0 b_0^{-1} + 1, \mathbb{Z}_{p^{n-r}})$ if b_0 is a unit. In summary, if the discriminant of C is a multiple of p, then C takes the form $p^r[uC(1, x, \mathbb{Z}_{p^{n-r}})]$, where $\gcd(u, p) = 1$ and either $r \geq 1$ or $x^2 - x - 1 \equiv 0 \pmod{p}$.

Suppose that the discriminant of $C = C(a, b, \mathbb{Z}_{p^n})$ is not a multiple of p. Then either a or b is relatively prime to p. Similar to the above, C takes the from $uC(1, t, \mathbb{Z}_{p^n})$, where $\gcd(t^2 - t - 1, p) = \gcd(u, p) = 1$. By Lemma 2.15, each one of them has $k(p^n)$ elements. Note that if $t = 0$, then $uC(1, 0, \mathbb{Z}_{p^n}) = uC(0, 1, \mathbb{Z}_{p^n})$.

3.1. Throughout the section, p is a prime of the form $5k \pm 2$. The following lemma is clear.

Lemma 3.2. *Let* p *be a prime of the form* $5k \pm 2$. *Then* $FS(p)$ *has* $(p^2 - 1)/k(p)$ *Fibonacci cycles. The discriminant of every cycle of* $FS(p)$ *is relatively prime to* p. *There are* $(p - 1)/\beta(p)$ *inequivalent cycles possess zeros. Each such cycle has* $\beta(p)$ *zeros. The remaining cycles possess no zeros.*

Proof. Since $p = 5k \pm 2$, $x^2 - x - 1 \equiv 0 \pmod{p}$ has no solution. Following Discussion 3.1, the discriminant of $C(a, b, \mathbb{Z}_p) \in FS(p)$ is not a multiple of p. By Lemma 2.15, $k(a, b, \mathbb{Z}_p) = k(p)$, $\alpha(a, b, \mathbb{Z}_p) = \alpha(p)$. Hence $FS(p)$ has $(p^2 - 1)/k(p)$ Fibonacci cycles. A cycle possesses zero takes the form $uC(0, 1, \mathbb{Z}_p)$, where $\gcd(u, p) = 1$. Each such cycle has $\beta(p)$ zero. This completes the proof of the lemma. □

We shall now study $FS(p^n)$. Since $p = 5k \pm 2$, $x^2 - x - 1 \equiv 0 \pmod{p}$ has no solution. Following Discussion 3.1, one has

(i) if the discriminant of $C = C(a, b, \mathbb{Z}_{p^n})$ is a multiple of p, then C takes the form $p[S] = (px_1, px_2, \cdots, px_t)$, where $S = (x_1, x_2, \cdots, x_t)$ is a member of $FS(p^{n-1})$,
(ii) if the discriminant of $C = C(a, b, \mathbb{Z}_{p^n})$ is not a multiple of p, C takes the from $uC(1, t, \mathbb{Z}_{p^n})$, where $\gcd(u, p) = 1$.

Among cycles with discriminant $\pm d$, where $\gcd(d,p)=1$, there are $\phi(p^n)/\beta(p^n)$ inequivalent cycles that contains zero. One may now determine $FS(p^n)$. See Example 4.3 for the case $p=3$.

3.2. Throughout the section, p is a prime of the form $5k\pm 1$. This implies that $x^2-x-1\equiv 0 \pmod p$ has two solutions. By Discussion 3.1,

(i) if the discriminant of $C=C(a,b,\mathbb{Z}_{p^n})$ is a multiple of p, then C takes the form $p[S]=(px_1,px_2,\cdots,px_t)$, where $S=(x_1,x_2,\cdots,x_t)$ is a member of $FS(p^{n-1})$, or $C=rC(1,b,\mathbb{Z}_{p^n})$, where $b^2-b-1\equiv 0 \pmod p$,

(ii) if the discriminant of $C=C(a,b,\mathbb{Z}_{p^n})$ is not a multiple of p, then C takes the from $uC(1,t,\mathbb{Z}_{p^n})$, where t is not a root of $x^2-x-1\equiv 0 \pmod p$ and $\gcd(u,p)=1$.

Among cycles with discriminant $\pm d$, where $\gcd(d,p)=1$, there are $\phi(p^n)/\beta(p^n)$ inequivalent cycles that contains zero.

3.3. The prime 5 is special among all the primes in the sense that $k(p^n)$ is a multiple of p^n if and only if $p=5$ (see Appendix A). $x^2-x-1\equiv 0 \pmod{5^n}$ is solvable if and only if $n=1$. Description of cycles can be obtained from (i) and (ii) of subsection 3.2 (replace p by 5). Among cycles with discriminant $\pm d$, where $\gcd(d,5)=1$, there are $\phi(5^n)/\beta(5^n)=5^{n-1}$ inequivalent cycles that contains zero. Note that $k(5^n)=4\cdot 5^n$, $\alpha(5^n)=5^n$ (see Appendix A).

4. Group Action

Let $C(a,b,\mathbb{Z}_m)=(E_1,E_2,\cdots)$. Recall that two adjacent terms (E_i,E_{i+1}) is called a pair of $C(a,b,\mathbb{Z}_m)$. A pair $(c,d)\in C(a,b,\mathbb{Z}_m)$ is called a multiple of (a,b) if

$$(c,d)=e(a,b),\ \text{where } e\in\mathbb{Z}_m \text{ is a unit..} \tag{4.1}$$

For each $r\in\mathbb{Z}_m^\times$, we define a map $f_r : FS(m)\to FS(m)$ by $f_r(C)=rC$ (see Lemma 2.7). Denoted by $S_{FS(m)}$ the symmetric group on $FS(m)$. Then the map $f : \mathbb{Z}_m^\times \to S_{FS(m)}$ defined by $f(r)=f_r$ is a group homomorphism. For each $C\in FS(m)$, the *stabiliser* of C is the subgroup $STAB(C)=\{r\in\mathbb{Z}_m^\times : rC=C\}$. The *orbit* of C is the set $O(C)=\{rC : r\in\mathbb{Z}_m^\times\}$ Note that members in $STAB(C)$ must leave the discriminant invariant. It follows that $r\in STAB(C)$ only if

$$r^2(b^2-ab-b^2)\equiv\pm(b^2-ab-a^2) \pmod m. \tag{4.2}$$

Among all the orbits, $O(C(0,1,\mathbb{Z}_m))$ is the one of special interest since $C_1=C(0,1,\mathbb{Z}_m)=C(1,1,\mathbb{Z}_m)$ is just the Fibonacci numbers modulo m. We shall call it the *fundamental Fibonacci cycle*. It is a Fibonacci cycle of discriminant ± 1. C_1 consists of $t=\beta(m)$ pairs that are multiples of $(0,1)$. C_1 takes the form

$$(0,a_1=1,a_1=1,\cdots,a_2,0,a_2,a_2,\cdots,a_3,0,a_3,a_3,\cdots,a_t,0,a_t,a_t,\cdots).$$

Hence $C(0,1,\mathbb{Z}_m)=C(1,1,\mathbb{Z}_m)=C(a_1,a_1,\mathbb{Z}_m)=\cdots=C(a_t,a_t,\mathbb{Z}_m)$. By Lemma 2.10, we have $a_i^2\equiv\pm 1 \pmod m$ and $t=\beta(m)\le 4$ (Lemma 2.15). Further,

$$STAB(C_1)=\{a_1,a_2,\cdots a_t\}. \tag{4.3}$$

It is a group of order $\beta(m)$. The orbit $O(C_1)$ consists $v=\phi(m)/\beta(m)$ members. To be more accurate, let $\mathbb{Z}_m^\times=\cup_{i=1}^v x_i STAB(C_1)$, then

$$O(C_1) = \{x_1C_1, x_2C_1, \cdots, x_vC_1\}. \tag{4.4}$$

In general, $C(a, b, \mathbb{Z}_m))$ may not consist of zeros ($C(1, 3, \mathbb{Z}_5) = \{1, 3, 4, 2\}$, the Lucas numbers modulo 5 has no zero). However, one may still determine the stabiliser $STAB(C(a, b, \mathbb{Z}_m))$ as follows. Let $(a_1a, a_1b) = (a, b), (a_2a, a_2b), \cdots, (a_ta, a_tb)$ be all the pairs of $C(a, b, \mathbb{Z}_m))$ that are the multiples of the pair (a, b). Note that $t = \beta(a, b, \mathbb{Z}_m)$ and that the a_i's are units (see Definition 2.3).

$$C(a, b, \mathbb{Z}_m) = (a, b, \cdots, a_2a, a_2b, \cdots, a_3a, a_3b, \cdots\cdots, a_ta, a_tb, \cdots). \tag{4.5}$$

(4, 5) implies that $a_i^{-1}C(a, b, \mathbb{Z}_m) = C(a, b, \mathbb{Z}_m) = a_iC(a, b, \mathbb{Z}_m)$. It follows that

$$STAB(C(a, b, \mathbb{Z}_m)) = \{a_1, a_2, \cdots, a_t\}. \tag{4.6}$$

The orbit $O(C(a, b, \mathbb{Z}_m))$ can be determined accordingly. It consists of $\phi(m)/t$ terms, where $t = \beta(a, b, \mathbb{Z}_m)$ is the number of pairs of $C(a, b, \mathbb{Z}_m)$ that are multiples of (a, b). In the case $\gcd(b^2 - ab - a^2, m) = 1$, $t = \beta(a, b, \mathbb{Z}_m) = \beta(m)$, which can be seen from Lemma 2.15. In the case $\gcd(b^2 - ab - a^2, m) \neq 1$, the order of $STAB(C(a, b, \mathbb{Z}_m))$ can be quite large (see Lemma 2.17 and Example 4.4). In summary, we have the following.

Lemma 4.1. *Let $C = C(a, b, \mathbb{Z}_m) \in FS(m)$ be a Fibonacci cycle. Then*

(i) *The stabiliser $STAB(C)$ is a subgroup of $\mathbb{Z}_m^\times$ of order $\beta(a, b, Z_m)$. Suppose $gcd\,(b^2 - ab - a^2, m) = 1$. Then $\beta(m) = \beta(a, b, \mathbb{Z}_m)$ is a divisor of 4.*

(ii) *The orbit $O(C) \in FS(m)$ has $\phi(m)/\beta(a, b, \mathbb{Z}_m)$ members, where $\phi(m)$ is the Euler function.*

.

Example 4.2. Let p be a prime of the form $5r \pm 2 \pmod 5$. Then $x^2 - x - 1 \equiv 0 \pmod p$ has no solution. It follows that every Fibonacci cycle in $FS(p)$ has nonzero discriminant. By Lemma 2.15, every Fibonacci cycle has $k(p)$ elements. $O(C)$ has $\phi(p)/\beta(p)$ members and $FS(p)$ has altogether $(p^2 - 1)/k(p)$ cycles.

Example 4.3. We study the Fibonacci system $FS(3^n)$ in detail as follows. It is known that $C_1 = C(0, 1, \mathbb{Z}_{3^n})$ has $k(3^n) = 8 \cdot 3^{n-1}$ members (see Lemma A1 of Appendix A). by Remark 2.16, $\beta(3^n) = 2$. By Lemma 4.1, $STAB(C(0, 1, \mathbb{Z}_{3^n}) = \langle \pm 1 \rangle$. Let $1 \leq r \leq 3^n/2$ be chosen such that $\gcd(r, 3) = 1$ and let $C_r = rC(0, 1, \mathbb{Z}_{3^n})$ (see Lemma 2.7). By Lemma 4.1, $O(C_1)$ has $\phi(3^n)/2$ members and $O(C_1) = \{C_r : 1 \leq r \leq 3^n/2, gcd(r, 3) = 1\}$. The only Fibonacci cycle C_r with discriminant ± 1 is C_1. Let S be a Fibonacci cycle of $\mathbb{Z}_{3^{n-1}}$ ($FS(\mathbb{Z}_{3^{n-1}})$ has $3^{2(n-1)} - 1$ terms). Then $3[S] = (3 \cdot x \,|\, x \in S)$ is a Fibonacci cycle of $\mathbb{Z}_{3^n}$ with discriminant $\pm 3^2 d$, where $\pm d$ is the discriminant of S (see Example 2.8). Note that $\pm 3^2 d \not\equiv 1 \pmod{3^n}$. Note also that the above mentioned Fibonacci cycles are not equivalent to one another and that the total number of terms is

$$8 \cdot 3^{n-1} \cdot \phi(3^n)/2 + 3^{2(n-1)} - 1 = 3^{2n} - 1,$$

where $\phi(x)$ is the Euler function. It follows that the above gives the Fibonacci system for $\mathbb{Z}_{3^n}$. C_1 is the only Fibonacci cycle with discriminant ± 1 as the discriminants of C_r ($r \neq 1$) and $3[S]$ are not ± 1.

Example 4.4. Let p be prime of the form $5k \pm 1$. By our results in subsection 3.2, the cycles of discriminant 0 take the form $rC(1, b_1, \mathbb{Z}_p)$ or $sC(1, b_2, \mathbb{Z}_p)$, where b_i are the roots of $x^2 - x - 1 \equiv 0 \pmod{p}$. The remaining cycles have nonzero discriminant, every one of them has $k(p)$ elements and takes the form $tC(1, b, \mathbb{Z}_p)$, where $b^2 - b - 1 \not\equiv 0 \not\equiv t \pmod{p}$. Let $p = 11$. The fundamental Fibonacci cycle $C_1 = C(0, 1, \mathbb{Z}_{11})$ consists only one 0. By Lemma 4.1, $O(C_1)$ has 10 members. 4 and 8 are solutions of $x^2 - x - 1 \equiv 0 \pmod{11}$ and the Fibonacci cycles of discriminant 0 are $C(1, 8, \mathbb{Z}_{11})$, $C(1, 4, \mathbb{Z}_{11})$, $2C(1, 4, \mathbb{Z}_{11})$. It follows that

$$FS(11) = C_1 \cup C_2 \cup \cdots \cup C_{10} \cup C(1, 8, \mathbb{Z}_{11}) \cup C(1, 4, \mathbb{Z}_{11}) \cup 2C(1, 4, \mathbb{Z}_{11}),$$

where $C_r = rC(0, 1, \mathbb{Z}_{11}) \in O(C_1)$. Note that the last two Fibonacci cycles have 5 terms and the rest have 10 terms. The stabiliser $STAB(C(1, 8, \mathbb{Z}_{11})) \cong \mathbb{Z}_{11}^{\times}$ is of order 10 (Lemma 2.17).

5. Representatives of the orbits $O(C)$

Let $C \in FS(p^n)$, where p is a prime. Applying our results in section 3, C takes the form $p[S]$, where $S \in FS(p^{n-1})$ or $rC(1, b, \mathbb{Z}_{p^n})$, where $\gcd(r, p) = 1$ (note that $rC(0, 1, \mathbb{Z}_{p^n}) = rC(1, 1, \mathbb{Z}_{p^n})$). We shall called a cycle of the form $rC(1, b, \mathbb{Z}_{p^n})$, where $\gcd(r, p) = 1$, a *primitive* Fibonacci cycle of $FS(p^n)$. It follows from the above discussion that every orbit O of $FS(p^n)$ has a representative R, where either R is a primitive cycle of $FS(p^n)$ or $R = p^m[S]$, where S is a primitive cycle of $FS(p^{n-m})$ for some $m \geq 1$. The following is clear.

Lemma 5.1. *If S_1 and S_2 are not in the same orbit of $FS(p^{n-1})$. Then $p[S_1]$ and $p[S_2]$ are not in the same orbit of $FS(p^n)$.*

Example 4.4 gives the cycles of $FS(11)$. The following gives representatives of orbits of $FS(121)$.

Example 5.2. Let $a = 4, 8$. $11k + a \in \mathbb{Z}_{121}$ $(0 \leq k \leq 10)$ are roots of $x^2 - x - 1 \equiv 0 \pmod{11}$. Among those roots, 37 and 85 are roots of $x^2 - x - 1 \equiv 0 \pmod{121}$. The representatives for orbits are

(i) The representatives from $FS(11)$. They are $11[C(0, 1, \mathbb{Z}_{11})]$, $11[C(1, 4, \mathbb{Z}_{11})]$ and $11[C(1, 8, \mathbb{Z}_{11})]$.
(ii) The representative that has its discriminant relatively prime to 11. There is only one such orbit with representative $C(0, 1, \mathbb{Z}_{121})$.
(iii) The representatives of discriminant 0. $C(1, 37, \mathbb{Z}_{121})$ and $C(1, 85, \mathbb{Z}_{121})$.
(iv) The representatives of discriminant $11k$ where $\gcd(11, k) = 1$. They are $C(1, 4, \mathbb{Z}_{121})$ and $C(1, 8, \mathbb{Z}_{121})$.

6. Residue completeness of $C(a, b, \mathbb{Z}_m)$

Definition 6.1. A Fibonacci cycle is called *residue complete* (nondefective) if $x \in C(a, b, \mathbb{Z}_m)$ for all $x \in \mathbb{Z}_m$.

Remark. Denoted by $\Omega(a, b, m)$ the collection of all distinct elements in $C(a, b, \mathbb{Z}_m)$. It is clear that $C(a, b, \mathbb{Z}_m)$ is residue complete if and only if $\mathbb{Z}_m = \Omega(a, b, m)$. Note that $\Omega(a, b, m)$ is a set while $C(a, b, \mathbb{Z}_m)$ is an ordered cycle.

Lemma 6.2. *Suppose that $C = C(a, b, \mathbb{Z}_m)$ is residue complete. Then $gcd(b^2 - ab - a^2, m) = 1$ and $C = rC(0, 1, \mathbb{Z}_m)$, where $gcd(r, m) = 1$.*

Proof. Since $C = C(a, b, \mathbb{Z}_m)$ is residue complete, $0 \in C$. By lemma 2.12, $C = rC(0, m_0, \mathbb{Z}_m)$, where $\gcd(r, m) = 1$ and the set of prime divisors of m_0 is a subset of the set prime divisors of m. Since $1 \in rC(0, m_0, \mathbb{Z}_m)$, one must have $m_0 = \pm 1$. Replace r by $-r$ if necessary, we have $C = rC(0, 1, \mathbb{Z}_m)$. The discriminant of C is $\pm(b^2 - ab - a^2) = \pm r^2$. Hence $\gcd(b^2 - ab - a^2, m) = 1$. □

Lemma 6.3. Let p be a prime. Then

(i) $C(a, b, \mathbb{Z}_p)$ is residue complete if $p = 2, 3, 5, 7$ and $\gcd(b^2 - ab - a^2, p) = 1$.
(ii) $C(a, b, \mathbb{Z}_8)$ and $C(a, b, \mathbb{Z}_{49})$ are not residue complete.

Proof. (i) Suppose that $C(a, b, \mathbb{Z}_p)$ is residue complete. By Lemma 6.2, such Fibonacci cycle takes the form $rC(0, 1, \mathbb{Z}_p)$, where $\gcd(r, p) = 1$. Hence $C(a, b, \mathbb{Z}_p)$ is residue complete only if $C(0, 1, \mathbb{Z}_p)$ is residue complete. Applying results of [B], $p = 2, 3, 5$ or 7. (ii) Suppose that $C = C(a, b, \mathbb{Z}_m)$ is residue complete, where $m = 8$ or 49. Then $0 \in C$. This implies that $C = rC(0, 1, \mathbb{Z}_m)$ for some r (Lemma 6.2). It follows that $C(0, 1, \mathbb{Z}_m)$ is residue complete. Recall that $C(0, 1, \mathbb{Z}_m)$ is just the Fibonacci numbers modulo m. Direct calculation shows that Fibonacci numbers modulo m ($m = 8, 49$) is not residue complete. □

In [B], there is some misprint in the proof of Lemma 2 as $2^2 + 2b - b^2 \equiv -1 \pmod{3^n}$ (see page 501 of [B]) is solvable for $n = 1$ but not solvable for $n = 2$. The following offers an alternative.

Lemma 6.4. *$C(v, u, \mathbb{Z}_{3^n})$ is residue complete if and only if $\gcd(u^2 - uv - v^2, 3) = 1$.*

Proof. Suppose that $C(v, u, \mathbb{Z}_{3^n})$ is residue complete. By Lemma 6.2, $\gcd(u^2 - uv - v^2, 3) = 1$.

We shall now prove the converse. Let $a \in \mathbb{N}$. We shall prove first by induction that there exists some b such that $b^2 - ab - a^2 \equiv \pm 1 \pmod{3^r}$ for all r.

Suppose that $a \equiv 1, 2 \pmod 3$. Then $x^2 - ax - a^2 \equiv -1 \pmod 3$ is solvable. Suppose that $x \equiv b \pmod{3^n}$ is a solution of $x^2 - ax - a^2 \equiv -1 \pmod{3^n}$. Then

$$b^2 - ab - a^2 = 3^n A - 1. \tag{6.1}$$

Let $x = 3^n t + b$. Then

$$x^2 - ax - a^2 \equiv 3^n t(2b - a) + 3^n A - 1 \pmod{3^{n+1}}. \tag{6.2}$$

Hence $x^2 - ax - a^2 \equiv -1 \pmod{3^{n+1}}$ is solvable if and only if

$$t(2b - a) + A \equiv 0 \pmod 3. \tag{6.3}$$

is solvable. But $2b - a \not\equiv 0 \pmod 3$, for otherwise equation (6.1) becomes

$$-5b^2 \equiv -1 \pmod 3, \tag{6.4}$$

which is not solvable. Hence $x^2 - ax - a^2 \equiv -1 \pmod{3^r}$ is solvable for all $r \geq 1$. In the case $a \equiv 0 \pmod 3$, we consider the equation

$$x^2 - ax - a^2 \equiv 1 \pmod{3^n}. \tag{6.5}$$

To show it is solvable, we apply mathematical induction. It is clear that the equation is solvable for $n = 1$. Suppose that $x \equiv b \pmod{3^n}$ is a solution of (6.5). Then

$$b^2 - ab - a^2 = 3^n A + 1. \tag{6.6}$$

Let $x = 3^n t + b$. Then

$$x^2 - ax - a^2 \equiv 3^n t(2b - a) + 3^n A + 1 \pmod{3^{n+1}}. \tag{6.7}$$

Hence $x^2 - ax - a^2 \equiv 1 \pmod{3^{n+1}}$ is solvable if and only if

$$t(2b - a) + A \equiv 0 \pmod 3. \tag{6.8}$$

is solvable. But $2b - a \not\equiv 0 \pmod 3$, for otherwise $2b \equiv a \equiv 0 \pmod 3$, and equation (6.6) becomes

$$0 \equiv -5b^2 \equiv 1 \pmod 3. \tag{6.9}$$

Hence $x^2 - ax - a^2 \equiv 1 \pmod{3^r}$ is solvable for all $r \geq 1$.

It follows that for any a, there exists b such that $C(a, b, \mathbb{Z}_{3^n})$ is a Fibonacci cycle of discriminant ± 1. By Example 4.3, the only Fibonacci cycle of discriminant ± 1 is $C(0, 1, \mathbb{Z}_{3^n})$. Hence $C(a, b, \mathbb{Z}_{3^n}) = C(0, 1, \mathbb{Z}_{3^n})$. It follows that $a \in C(0, 1, \mathbb{Z}_{3^n})$ for all $a \in \mathbb{Z}_{3^n}$. Hence $C(0, 1, \mathbb{Z}_{3^n})$ is residue complete. Finally, one sees from Example 4.3 again that any Fibonacci cycle $C(v, u, \mathbb{Z}_{3^n})$ with $\gcd(\ u^2 - uv - v^2, 3) = 1$ must take the form $rC(0, 1, \mathbb{Z}_{3^n})$, where $\gcd(r, 3) = 1$. Hence $C(v, u, \mathbb{Z}_{3^n})$ is residue complete. □

The following generalises Lemma 3 of Burr ([B]). The idea of the proof, however, is the same.

Lemma 6.5. *Suppose that $gcd(b^2 - ab - a^2, 5) = 1$, $C(a, b, \mathbb{Z}_m)$ is residue complete and $k(a, b, \mathbb{Z}_m) = r$, $k(a, b, \mathbb{Z}_{5m}) = 5r$. Then $C(a, b, \mathbb{Z}_{5m})$ is residue complete.*

Proof. Since $C(a, b, \mathbb{Z}_m)$ is residue complete, $\gcd(b^2 - ab - a^2, m) = 1$ (Lemma 6.2). It follows by our assumption that $\gcd(b^2 - ab - a^2, 5m) = 1$. This implies that $k(a, b, \mathbb{Z}_5) = k(5), k(a, b, \mathbb{Z}_m) = k(m)$, and $k(a, b, \mathbb{Z}_{5m}) = k(5m)$ (Lemma 2.15). To show $C(a, b, \mathbb{Z}_{5m})$ is residue complete, define the map

$$f : \Omega(a, b, 5m) \to \Omega(a, b, m) \tag{6.10}$$

by $f(x) = x \pmod m$ (see remark of Definition 6.1 for notation). If one can show that every member x in $C(a, b, \mathbb{Z}_m)$ has 5 preimages, then $C(a, b, \mathbb{Z}_{5m})$ is residue complete.
(i) Suppose that $\gcd(5, m) = 1$. By our assumption, $5r = k(5m) = lcm(k(5), k(m))$ $= lcm(20, k(m))$ (see Appendix A). Hence r is a multiple of 4. For each $x \in C(a, b, \mathbb{Z}_m)$, let $E_s \in C(a, b, \mathbb{Z}_{5m})$ be chosen such that $E_s \equiv x \pmod m$. We now consider $E_s, E_{r+s}, E_{2r+s}, E_{3r+s}, E_{4r+s} \in C(a, b, \mathbb{Z}_{5m})$. Since $k(a, b, \mathbb{Z}_m) = r$, one has $E_s \equiv E_{r+s} \equiv E_{2r+s} \equiv E_{3r+s} \equiv E_{4r+s} \pmod m$. Hence

$$x = f(E_s) = f(E_{r+s}) = f(E_{2r+s}) = f(E_{3r+s}) = f(E_{4r+s}). \tag{6.11}$$

We now consider $E_s, E_{r+s}, E_{2r+s}, E_{3r+s}, E_{4r+s}$ modulo 5. Since $FS(5) = C(0, 1, \mathbb{Z}_5)$ $\cup C(1, 3, \mathbb{Z}_5)$, $\gcd(b^2 - ab - a^2, 5) = 1$, we have $F(a, b, \mathbb{Z}_{5m}) \equiv F(0, 1, \mathbb{Z}_5)$ modulo 5 (see (2.1) for notation). Note that $C(0, 1, \mathbb{Z}_5)$ is given by

$$C(0, 1, \mathbb{Z}_5) = (0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1).$$

Denoted by x_r the elements in $F(0, 1, \mathbb{Z}_5)$. An easy observation of $C(0, 1, \mathbb{Z}_5)$ shows that

(A) $x_v \not\equiv x_{4u+v} \pmod 5$ for any $u, v \in \mathbb{Z}$.

Since r is a multiple of 4 and $F(a,b,\mathbb{Z}_{5m}) \equiv F(0,1,\mathbb{Z}_5)$ modulo 5, (A) of the above implies that the 5 members $E_s, E_{r+s}, E_{2r+s}, E_{3r+s}, E_{4r+s}$ are not congruent to one another modulo 5. Hence every member x in $\Omega(a,b,m)$ has 5 distinct preimages (see (6.10)) $E_s, E_{r+s}, E_{2r+s}, E_{3r+s}, E_{4r+s}$ in $\Omega(a,b,5m)$. Since $C(a,b,\mathbb{Z}_m)$ is residue complete, $C(a,b,\mathbb{Z}_{5m})$ is also residue complete.
(ii) Suppose that $5|m$. It follows that $4|k(m) = r$ (see Appendix A). For each $a_0 \in C(a,b,\mathbb{Z}_m)$, let $E_s \in C(a,b,\mathbb{Z}_{5m})$ be chosen such that $E_s \equiv a_0 \pmod m$. We now consider $E_s, E_{r+s}, E_{2r+s}, E_{3r+s}, E_{4r+s} \in C(a,b,\mathbb{Z}_{5m})$. Since $k(a,b,\mathbb{Z}_m) = r$, one has $E_s \equiv E_{r+s} \equiv E_{2r+s} \equiv E_{3r+s} \equiv E_{4r+s} \pmod m$. Hence

$$a_0 = f(E_s) = f(E_{r+s}) = f(E_{2r+s}) = f(E_{3r+s}) = f(E_{4r+s}). \tag{6.12}$$

By (2.4), one has

$$V_{tr+s} = \begin{pmatrix} E_{tr+s+1} & E_{tr+s} \\ E_{tr+s} & E_{tr+s+1} - E_{tr+s} \end{pmatrix} = \begin{pmatrix} b & a \\ a & b-a \end{pmatrix} \sigma^{tr+s-1}, \tag{6.13}$$

where $0 \le t \le 4$. Let $E_{s+1} \equiv b_0 \pmod m$. Since $k(a,b,\mathbb{Z}_m) = k(m) = r$, we have

$$V_s \equiv V_{r+s} \equiv V_{2r+s} \equiv V_{3r+s} \equiv V_{4r+s} \equiv \begin{pmatrix} b_0 & a_0 \\ a_0 & b_0 - a_0 \end{pmatrix} \pmod m. \tag{6.14}$$

Applying (6.14) of the above, V_{tr+s} $(0 \le t \le 4)$ modulo $5m$ take the following form

$$V_{tr+s} \equiv \begin{pmatrix} xm + b_0 & ym + a_0 \\ ym + a_0 & xm + b_0 - (ym + a_0) \end{pmatrix} \pmod{5m}. \tag{6.15}$$

We now calculate the determinant of V_{tr+s} is different ways.

(i) Since $4|r$ and $\det \sigma = -1$, applying (6.13) of the above, one has $\det V_{tr+s} = D = \pm(b^2 - ab - a^2)$ in $\mathbb{Z}$.
(ii) $\det V_{tr+s} = b_0^2 - a_0 b_0 - a_0^2$ modulo m (see (6.14)).
(iii) $\det V_{tr+s} = (xm + b_0)^2 - (xm + b_0)(ym + a_0) - (ym + a_0)^2$ modulo $5m$ (see (6.15) of the above).

We now investigate (i)-(iii) as follows. Applying (i) and (ii) of the above, one has

$$b_0^2 - a_0 b_0 - a_0^2 \equiv Am + D \pmod{5m} \tag{6.16}$$

for some integer A. Applying (i), (iii) and (6.16) of the above, one has

$$m^2(x^2 - y^2 - xy) - my(2a_0 + b_0) + mx(2b_0 - a_0) + mA \equiv 0 \pmod{5m}. \tag{6.17}$$

Since $5|m$, one must have $-(2a_0 + b_0)y + (2b_0 - a_0)x + A \equiv 0 \pmod 5$. Note that $2b_0 - a_0 \not\equiv 0 \pmod 5$, for otherwise

$$0 \not\equiv \pm(b^2 - ab - a^2) \equiv b_0^2 - a_0 b_0 - a_0^2 \equiv -5b_0 \equiv 0 \pmod 5.$$

Similarly, $2a_0 + b_0 \not\equiv 0 \pmod 5$. Hence

$$x \equiv \frac{-A + (2a_0 + b_0)y}{2b_0 - a_0},\ y \equiv \frac{A + (2b_0 - a_0)x}{2a_0 + b_0} \pmod 5. \tag{6.18}$$

For any $E_{t_1 r+s}$, $E_{t_2 r+s}$, by (6.15), they take the form $y_1 m + a_0$ and $y_2 m + a_0$. By (6.15), $E_{t_1 r+s+1}$ and $E_{t_2 r+s+1}$ take the form $x_1 m + b_0$ and $x_2 m + b_0$. Suppose that

$$E_{t_1 r+s} \equiv E_{t_2 r+s} \pmod{5m}, \tag{6.19}$$

where $0 \le t_2 < t_1 \le 4$. Then $y_1 m + a_0 \equiv y_2 m + a_0 \pmod{5m}$. It follows that $y_1 \equiv y_2 \pmod 5$. Applying (6.18), $x_1 \equiv x_2 \pmod 5$. This implies that

$$E_{t_1 r+s+1} = x_1 m + b_0 \equiv x_2 m + b_0 = E_{t_2 r+s+1} \pmod{5m}. \tag{6.20}$$

Since $\gcd(b^2 - ab - a^2, 5m) = 1$, it follows from (6.13), (6.19) and (6.20) that

$$\sigma^{(t_1 - t_2)r} \equiv I \pmod{5m}, \tag{6.21}$$

where $0 \le t_2 < t_1 \le 4$. In particular, $5r = k(5m) \le (t_1 - t_2)r \le 4r$. A contradiction. Hence (6.19) is false. Equivalently, $E_{t_1 r+s} \not\equiv E_{t_2 r+s}$ modulo $5m$ for $t_1 \ne t_2$. This implies that $E_s, E_{r+s}, E_{2r+s}, E_{3r+s}, E_{4r+s}$ modulo $5m$ give 5 distinct numbers. Consequently, every member a_0 in $\Omega(a, b, m)$ has 5 preimages (see (6.10) and (6.12)) $E_s, E_{r+s}, E_{2r+s}, E_{3r+s}, E_{4r+s}$ in $\Omega(a, b, 5m)$. Since $C(a, b, \mathbb{Z}_m)$ is residue complete, $C(a, b, \mathbb{Z}_{5m})$ is also residue complete. □

7. The Main Result

It is clear that if $C(a, b, \mathbb{Z}_n)$ is not residue complete, then $C(a, b, \mathbb{Z}_{mn})$ is not residue complete. Lemma 6.5 implies that if $C(a, b, \mathbb{Z}_n)$ is residue complete, then $C(a, b, Z_{5^b n})$ (with appropriate assumptions) is residue complete. These two facts together with Lemmas 6.3, 6.4 and some simple calculation imply that the $C(0, 1, \mathbb{Z}_n)$ is residue complete if and only if $n \in RS = \{5^k, 2 \cdot 5^k, 4 \cdot 5^k, 3^j 5^k, 6 \cdot 5^k, 7 \cdot 5^k, 14 \cdot 5^k \mid k \ge 0, j \ge 1\}$. This was first achieved by S.A. Burr [B] in his 1971 article which gave some very neat insights about the Fibonacci systems. A simple study of the Fibonacci systems actually gives us the following.

Lemma 7.1. *The Lucas numbers $C(1, 3, \mathbb{Z}_m)$ modulo m is residue complete if and only if $m = 2, 4, 6, 7, 14, 3^n$.*

Proof. Suppose that $C = C(1, 3, \mathbb{Z}_m)$ is residue complete. By Lemma 6.2, $\gcd(3^2 - 3 - 1, m) = 1$ and $C = rC(0, 1, \mathbb{Z}_m)$, where $\gcd(r, m) = 1$, $C(0, 1, \mathbb{Z}_m)$ is the Fibonacci numbers modulo m. Hence the Lucas numbers modulo m is residue complete only if the Fibonacci numbers modulo m is residue complete and $\gcd(m, 5) = 1$. By results of [B] (see the introduction of section 7), $m \in \{2, 4, 6, 7, 14, 3^c\}$. By Lemma 6.4, $C(1, 3, \mathbb{Z}_{3^c})$ is residue complete. Direct calculation shows that $C(1, 3, \mathbb{Z}_m)$ is residue complete if $m = 2$, 4, 6, 7, 14. This completes the proof. □

Proposition 7.2. *Let $a, b \in \mathbb{Z}$. Then $C(a, b, \mathbb{Z}_m)$ is residue complete if and only if*

(i) *$gcd(b^2 - ab - a^2, m) = 1$,*
(ii) *$m \in RS = \{5^k, 2 \cdot 5^k, 4 \cdot 5^k, 3^j 5^k, 6 \cdot 5^k, 7 \cdot 5^k, 14 \cdot 5^k \mid k \ge 0, j \ge 1\}$.*

Proof. Suppose that $C(a, b, \mathbb{Z}_m)$ is residue complete. By Lemma 6.2, $\gcd(b^2 - ab - a^2, m) = 1$ and $C(a, b, \mathbb{Z}_m) = dC(0, 1, \mathbb{Z}_m)$, where $\gcd(d, m) = 1$. Applying resuts of [B] (see the introduction of section 7), one has $m \in RS$.

Conversely, suppose that $C(a, b, \mathbb{Z}_m)$ satisfies (i) and (ii) of the above. In the case $\gcd(b^2 - ab - a^2, 5) = 5$, (i) and (ii) imply that $m \in \{2, 3, 4, 6, 7, 14, 3^n\}$. one can check easily that $C(a, b, \mathbb{Z}_m)$ is residue complete for $m = 2, 3, 4, 6, 7, 14$, as long as $\gcd(b^2 - ab - a^2, m) = 1$. By Lemma 6.4, $C(a, b, \mathbb{Z}_{3^n})$ is residue complete if $\gcd(a^2 - ab - b^2, 3) = 1$.

In the case $\gcd(b^2 - ab - a^2, 5) = 1$, one can check directly, with the help of Lemma 6.4, that $C(a, b, \mathbb{Z}_m)$ is residue complete for $m = 6, 14, 20, 3^n$ as long as

$\gcd(b^2-ab-a^2, m) = 1$. Applying Lemma 6.5, $C(a, b, \mathbb{Z}_m)$ is residue complete for $m \in RS$ as long as $\gcd(b^2-ab-a^2, m) = 1$. □

8. Appendix A

Applying Lemma 2.2, $k(m)$ is the order of σ modulo m. We shall reprove in the appendix some basic facts about $k(m)$.

Lemma A1. *$k(m)$ is the order of σ in $GL(2, \mathbb{Z}_m)$. Further, let p be a prime. Then*

(i) $k(2) = 3, k(3) = 8, k(4) = 6, k(5) = 20$.
(ii) *$k(p)|(p-1)$ if p is a prime of the form $5k \pm 1$.*
(iii) *$k(p)|2(p+1)$ if p is a prime of the form $5k \pm 2$.*
(iv) *Let t be the largest integer such that $k(p^t) = k(p)$. Then $k(p^r) = p^{r-t}k(p)$ for all $r \geq t$. Let t be the largest integer such that $\alpha(p^t) = \alpha(p)$. Then $\alpha(p^r) = p^{r-t}\alpha(p)$ for all $r \geq t$.*
(v) *Let p be a prime. Then p^e divides $k(p^e)$ if and only of $p = 5$. Further, $k(5^e) = 4 \cdot 5^e$, $k(2^e) = 3 \cdot 2^{e-1}$, $k(3^e) = 8 \cdot 3^{e-1}$.*

Proof. Note first that (v) is a direct consequence of (i)-(iv). (i) is easy. The characteristic polynomial of σ is $x^2 - x - 1$. The eigenvalues of σ are $(1 \pm \sqrt{5})/2$. Hence σ is similar to σ_0 in a finite field that contains $\sqrt{5}$, where

$$\sigma_0 = \begin{pmatrix} (1+\sqrt{5})/2 & 0 \\ 0 & (1-\sqrt{5})/2 \end{pmatrix}. \tag{A.1}$$

Proof of (ii). Since $p \equiv \pm 1 \pmod 5$, 5 is a square in $\mathbb{Z}_p^\times$. Hence the eigenvalues $(1 \pm \sqrt{5})/2$ of σ are members of $\mathbb{Z}_p^\times$. Since conjugation preserves the order, $k(m)$ is given by the order of σ_0. Note that the orders of $(1 \pm \sqrt{5})/2) \in \mathbb{Z}_p^\times$ are divisors of $p-1$. This implies that the order of σ is a divisor of $p-1$.

Proof of (iii). Since p is of the form $5k \pm 2$, 5 is not a square in $\mathbb{Z}_p$. Hence the eigenvalues $(1 \pm \sqrt{5})/2$ of σ are not members of $\mathbb{Z}_p$. Let $F = \mathbb{Z}_p[\sqrt{5}]$ be the Galois field of order p^2 that contains $(1 \pm \sqrt{5})/2$. Consider the map $f : F^\times \to \mathbb{Z}_p^\times$ defined by $f(a + b\sqrt{5}) = (a + b\sqrt{5})(a - b\sqrt{5})$. This is known as the norm map. The kernel of f is a subgroup of $F^\times$ that consists of all $x \in F^\times$ such that $f(x) = 1$. Since f is a surjective homomorphism, the kernel of f is a subgroup of order $p+1$. Since the norm of $((1+\sqrt{5})/2)^2$ is 1, $((1+\sqrt{5})/2)^2$ is in the kernel. Hence the order of $((1+\sqrt{5})/2)^2$ is a divisor of $p+1$. As a consequence, the order of σ_0 (see (A.1)), as well as σ, is a divisor of $2(p+1)$.

Proof of (iv). Suppose that p is odd. Let $k(p^t) = k(p) = e$. By our assumption

$$\sigma^e = I + p^t \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ where } \gcd(a, b, c, d, p) = 1. \tag{A.2}$$

Hence

$$\sigma^{pe} = \sum_{m=0}^{p} p^{tm} \begin{pmatrix} p \\ m \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^m. \tag{A.3}$$

One sees easily that $\sigma^{pe} \equiv I \pmod{p^{t+1}}$ and $\sigma^{pe} \not\equiv I \pmod{p^{t+2}}$ (p is odd). This implies that $k(p^r) = p^{r-t}k(p^t) = p^{r-t}k(p)$. In the case $p = 2$, one has $k(2) = 3$,

$k(4) = 6$ and that

$$\sigma^{2^{t-1}3} = I + 2^t \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ where } \gcd(a, b, c, d, 2) = 1. \tag{A.4}$$

It follows that $k(2^e) = 3 \cdot 2^{e-1}$. The second part of (iv) can be proved similarly. □

Remark. (iv) does not hold for $C(a, b, \mathbb{Z}_m)$ if $\gcd(b^2 - ab - a^2, m) \neq 1$ as the following shows. (a) $k(1, 4, \mathbb{Z}_{11}) = 5$, $k(1, 4, \mathbb{Z}_{121}) = 110 \neq 11k(1, 4, \mathbb{Z}_{11})$, $k(1, 4, \mathbb{Z}_{11^3}) = 1210$. (b) $\alpha(1, 4, \mathbb{Z}_{11}) = 1$, $\alpha(1, 4, \mathbb{Z}_{121}) = 10 \neq 11\alpha(1, 4, \mathbb{Z}_{11}) = 11$, $\alpha(1, 3, \mathbb{Z}_{25}) = 5 = 5\alpha(1, 3, \mathbb{Z}_5) = 5$.

Since $k(m)$ is the order of σ modulo m, the following is clear.

Lemma A2. *Suppose that* $gcd\,(m, n) = 1$. $k(mn) = k(m)k(n)/gcd\,(k(m), k(n))$.

The order of σ modulo m, in general, is not very easy to determine. Applying Lemma A1, one can get an upper bound for $k(p^e)$, where p is a prime. By Lemma A2, one can get an upper bound for $k(m)$. Consequently, one can show that $k(n) \leq 6n$. Further, the following holds.

(i) $k(n)/n \leq 6$, $k(n)/n = 6$ if and only if $n = 2 \cdot 5^f$, where $f \geq 1$,
(ii) $k(n)/n = 5$ has no solution,
(iii) $k(n)/n = 4$ if and only if $n = 2 \cdot 3 \cdot 5^a$ or 5^b, where $a \geq 0$, $b \geq 1$,
(iv) $k(n)/n = 1, 2, 3$ if and only if $n = 24 \cdot 5^e, 12 \cdot 5^e, 4 \cdot 5^f$ respectively, where $e \geq 0$, $f \geq 1$.

Proof of (i). Suppose that $k(n) = 6n$. Let $n = n_0 p^e$, $\gcd(n_0, p) = 1$, where p is the largest prime divisor of n. Suppose that $p \neq 2, 3$. Since $k(n) = 6n$, p^e is a divisor of $k(n)$ and p is the largest prime divisor of $k(n)$. Applying Lemma A1, the largest prime divisor of $k(q^e)$, where $q \geq 5$, is q or less. Hence the largest prime divisor of $k(n)$ must comes from $k(p^e)$. It follows that p^e is a divisor of $k(p^e)$. Applying (v) of Lemma A1, $p = 5$. As a consequence, n takes the form $2^a 3^b 5^c$. One sees easily that if $b \neq 0$, then $k(2^a 3^b 5^c)/2^a 3^b 5^c$ is not divisible by 3. A contradiction. Hence n must take the form $2^a 5^c$. One may now obtain the desired result by simple calculation. (ii)-(iv) can be proved similarly. □

Discussion. In (i)-(iv) of the above, n takes the form $r \cdot 5^e$, where r is a divisor 24. Note that the number 24 is special in the following sense.

$$\mathbb{Z}_r^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \text{ if and only if } r \text{ is a divisor of } 24.$$

9. Appendix B

In Example 2.5, $(4, 4) = x(2, 2)$ modulo 6 has two solutions 2, and 5. Following Definition 2.3, we choose $e = 5$. We will show in this appendix that if $(x, y) \in C(a, b, \mathbb{Z}_m)$ takes the form $e(a, b)$ for some $e \in \mathbb{Z}_m$, then one may always choose $e \in \mathbb{Z}_m$ to be a unit. Lemma B1 is clear.

Lemma B1. *Let* $C \in FS(m)$. *Then there exists a unique* $S \in FS(n)$ *for some* $n|m$ *such that*

(i) $C = d[S]$, *where* $d|m$, $S \in FS(n)$ *and* $m = dn$,
(ii) *if* $S = r[S_0]$ *for some* r, *then* $gcd\,(r, n) = 1$.

Lemma B2. *Let C and $S = C(r, s, \mathbb{Z}_n)$ be given as in Lemma B1. Suppose that $(t, u) \in C(r, s, \mathbb{Z}_n)$ takes the form $e(r, s)$ for some e. Then $gcd\,(e, n) = 1$.*

Proof. Suppose that $\gcd(e, n) = e_0 \neq 1$. Then $S = (r, s, \cdots, t = er, u = es, \cdots) = (ea, eb, e(a + b), \cdots) = e_0[S_0]$, for some S_0. Note that e_0 is not a unit in $\mathbb{Z}_n$. This contradicts (ii) of Lemma B1. Hence e must be a unit in $\mathbb{Z}_m$. □

Proposition B3 *Let $(x, y) \in C(a, b, \mathbb{Z}_m)$ be a multiple of (a, b). Then $(x, y) = e(a, b)$ for some e, where $e \in \mathbb{Z}_m$ is a unit.*

Proof. Let $C = d[S]$ (see Lemma B1). Then $S = (a/d, b/d, \cdots, x/d, y/d, \cdots)$. By our assumption, (x, y) is a multiple of (a, b). Hence $(x/d, y/d)$ is a multiple of $a/d, b/d)$. Applying Lemma B2, $(x/d, y/d) = e(a/d, b/d)$ modulo n for some e, where $\gcd(e, n) = 1$. It follows that $(x/d, y/d) = (e + zn)(a/d, b/d)$ modulo n for all $z \in \mathbb{Z}$. Hence $(x, y) = (e + zn)(a, b)$ modulo m for all $z \in \mathbb{Z}$.

Let p be a prime divisor of m. If $p|n$, since $\gcd(e, n) = 1$, $\gcd(e + zn, p) = 1$ for all $z \in \mathbb{Z}$. If $\gcd(p, n) = 1$, then $\gcd(e + u_p n, p) = 1$ for some u_p, since otherwise

$$p|gcd\,(e + sn, e + tn) \text{ for all } s, t \in \mathbb{Z},$$

which implies that $p|(s - t)$ for all $s, t \in \mathbb{Z}$. A contradiction. In summary, for each prime divisor p of m, there exists some u_p such that $\gcd(e + u_p n, p) = 1$. By Chinese Remainder Theorem, there exists some u such that $\gcd(e + un, m) = 1$ and $(x, y) = (e + un)(a, b)$ modulo m. □

References

[B] S. A. Burr, *On Moduli for which the Fibonacci sequence contains a complete system of residues*, Fibonacci Quaterly, 9(5), 497-504 (1971).

DEPARTMENT OF APPLIED MATHEMATICS,
I-SHOU UNIVERSITY,
KAOHSIUNG, TAIWAN,
REPUBLIC OF CHINA.

cllang@isu.edu.tw

lang2to46@gmail.com